I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

The Plain View Doctrine Strikes Out in Digital File Searches

MATTHEW DODOVICH*

Abstract: On April 8, 2004, federal agents raided two drug testing laboratories seeking information related to "anonymous" performance-enhancing drug tests administered to ten Major League Baseball players. The search was pursuant to a properly executed search warrant, which authorized the agents to obtain testing records and specimens for the ten named players. The lab also possessed drug-testing information on other players for whom the agents did not have permission to search, so the agents relied on the "plain view doctrine," an extension of the Fourth Amendment that allows investigators to search and seize items that are in "plain view" during a legal search. Investigators used information seized under the plain view doctrine to obtain search warrants for the records of over 100 athletes who had tested positive for steroids.

The Major League Baseball Players Association (MLBPA), on the players' behalf, sought return of all records discovered outside the scope of the warrant. After three district courts ruled for the MLBPA, the United States Court of Appeals for the Ninth Circuit reversed, holding that (1) the government had demonstrated a need to seize intermingled evidence for off-site review and its plan for sorting was approved by a magistrate, and (2) no rule exists that evidence turned up during a rightful search must

* Matt Dodovich is a Privacy Issues Editor and the Note Writing Coordinator for *I/S: A Journal of Law and Policy for the Information Society*, and a 2011 J.D. candidate at the Moritz College of Law at The Ohio State University. If there are two things that he loves, they are baseball and individual rights.

be excluded because it supports charges for a related crime not expressly stated in the warrant. An en banc panel of the Ninth Circuit reversed this decision, holding that the government had overstepped the warrant and the plain view doctrine in using the evidence it found to apply for more warrants.

Many federal and state courts have looked at the applicability of the plain view doctrine to digital file searches. This Note will analyze those cases, in addition to the Ninth Circuit's en banc decision. The Note will argue that the plain view doctrine should not generally apply to computer searches, as computers contain vast amounts of easily accessible information and are ripe for abuse by government investigators. Courts addressing this issue should remain true to the Fourth Amendment and the purposes of the plain view doctrine, and protect people's Fourth Amendment rights by generally prohibiting application of the plain view doctrine to electronically stored data.

I. INTRODUCTION

The plain view doctrine allows a government official, under the Fourth Amendment to the U.S. Constitution, to seize items without a warrant provided that the officer is lawfully present at the place where the evidence can be plainly viewed, the officer has a lawful right of access to the object, and the incriminating character of the object is immediately apparent.[1] The plain view doctrine has undergone significant changes since it was first articulated in the plurality opinion of *Coolidge v. New Hampshire*.[2] The police originally used the plain view doctrine to seize things such as stolen stereo equipment or illegal weapons found during a drug raid.[3] Over the last two decades, the advent and increased presence of new technologies—most notably personal computers—have brought into question how the plain view doctrine should apply to searches of digitally stored data and information.

---

[1] Horton v. California, 496 U.S. 128, 134 (1990).

[2] 403 U.S. 443, 465 (1971); *see Horton*, 496 U.S. at 138-41 (removing the requirement that evidence must be discovered "inadvertently"); *see also* Arizona v. Hicks, 480 U.S. 321, 327-28 (1987) (holding that a police officer could not turn a stereo in order to check its serial number to confirm that it was stolen).

[3] *See generally Hicks*, 480 U.S. 321; United States v. Tate, 133 F. App'x 447 (9th Cir. 2005).

One such attempt to apply the plain view doctrine to government searches of computer files took the field against the Major League Baseball Players Association (the "MLBPA").[4] In the 2000s, allegations began to surface that a significant number of the MLB's players were using performance-enhancing drugs ("PEDs"). Congress held hearings on the subject of steroids in baseball and eventually initiated investigations into the Bay Area Laboratory Co-Operative ("BALCO") and several MLB players.[5] Jose Canseco, a former MLB player, wrote a "tell-all" book that detailed, among other things, his use of steroids while an MLB player as well as that of several other players whom he "knew" to use steroids.[6] The MLB responded by instituting a "survey" level of drug testing in 2003, which was administered by Comprehensive Drug Testing Inc. ("CDT") and Quest Diagnostics Inc. ("Quest").[7] The specimens were stored at Quest under a number coding system, while the names were stored electronically at CDT.[8]

In November of 2003, the government began attempting to obtain the results of the MLB's drug tests.[9] To search CDT and Quest, the government procured warrants that authorized the seizure of information relating to ten named players with connections to BALCO.[10] Investigators confiscated and searched pieces of computer equipment, including one computer that contained the "Tracey" directory.[11] This directory contained information on eight of the ten players named in the warrant, as well as twenty-six other MLB players

---

[4] Major League Baseball ("The MLB") and the MLBPA are not strangers to the federal courts. *See* Fed. Baseball Club v. Nat'l League, 259 U.S. 200 (1922) (Finding the MLB exempt from the Sherman Antitrust Laws); Flood v. Kuhn, 407 U.S. 258 (1972) (Upholding *Federal Baseball Club*'s judgment, but questioning its rationale); Baltimore Orioles v. Major League Baseball Player's Ass'n, 805 F.2d 663 (7th Cir. 1986).

[5] Rebecca Shore, *How We Got Here: A Timeline of Performance-Enhancing Drugs in Sports*, SI.COM, Mar. 11, 2008, *available at* http://sportsillustrated.cnn.com/2008/magazine/03/11/steroid.timeline/index.html.

[6] *Id.*

[7] *See* United States v. Comprehensive Drug Testing, 513 F.3d 1085, 1090 (9th Cir. 2008).

[8] *Comprehensive Drug Testing*, 513 F.3d at 1093.

[9] *Id.* at 1090.

[10] *Id.* These 10 players' names were filed under seal and thus are not available. *Id.* at n.4.

[11] *Id.* at 1092.

and many other professional athletes.[12] Federal investigators eventually used this information to apply for warrants covering over 100 non-BALCO players who had tested positive for PEDs.[13]

The MLBPA filed motions in two district courts, seeking the return of the specimens and drug testing records of those players not specified in the original warrant.[14] The two courts granted the MLBPA's motions and ordered a return of the property.[15] The Government appealed the decisions of the district courts to the United States Court of Appeals for the Ninth Circuit, which led to the panel decision in *United States v. Comprehensive Drug Testing* (referred to as "*CDT*").[16] The *CDT* panel reversed the district courts' decisions, finding that the government's seizure of intermingled evidence for off-site review through the search warrant was lawful.[17] The MLBPA appealed, and an en banc panel of the Ninth Circuit reheard the case and reversed. A majority found the plain view doctrine inapplicable to computer searches and prescribed an alternate procedure that must be used by law enforcement when seeking information from a computer or other digital device.[18] The government petitioned for a rehearing of the en banc decision to the entire Ninth Circuit Court of Appeals.[19] In response, the Ninth Circuit rescinded its original opinion and issued a new opinion, which reached the same decision in the case, but moved some of the more controversial language from the majority opinion to a concurring opinion.[20]

This Note will explore *United States v. Comprehensive Drug Testing* as it pertains to the plain view doctrine and its application to government searches of computer files. The Ninth Circuit en banc decision and its concurring opinion by Chief Judge Alex Kozinski

---

[12] *Id.* at 1093.

[13] *Id.* at 1094.

[14] *Comprehensive Drug Testing*, 513 F.3d at 1094.

[15] *Id* at 1094-95.

[16] *Id.* at 1090.

[17] *Id.* at 1110-12.

[18] United States v. Comprehensive Drug Testing, 579 F.3d 989 (9th Cir. 2009) (en banc).

[19] Neither party petitioned for certiorari to the United States Supreme Court.

[20] United States v. Comprehensive Drug Testing, 621 F.3d 1162 (9th Cir. 2010) (en banc).

properly apply the plain view doctrine to computer searches.[21] Computers contain a lot of information that is easily searched and viewed. Past court decisions applying the plain view doctrine to computer file searches fail to recognize law enforcement officers' ability to abuse the scope of their warrants and unreasonably invade the privacy of citizens in violation of the Fourth Amendment. Future decisions by the courts should adhere to the wisdom and logic of the Ninth Circuit en banc opinion and the concurring opinion of Chief Judge Kozinski. Its analysis strikes the correct balance between law enforcement's need to execute searches and the need to protect the public's right to privacy.

II. AN OVERVIEW OF THE FOURTH AMENDMENT AND THE PLAIN VIEW DOCTRINE

The Fourth Amendment to the United States Constitution was adopted as part of the Bill of Rights in 1789[22] and incorporated to the states in its entirety in 1961.[23] The amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing* the place to be searched, and the persons or *things to be seized*.[24]

Thus, the Fourth Amendment has two distinct parts: (1) it protects against unreasonable searches and seizures by law enforcement, and (2) it provides that government searches must be accompanied by a

---

[21] Chief Judge Alex Kozinski's concurrence was originally part of the Ninth Circuit's en banc decision, but was changed to a concurrence when the opinion was reissued. This was because the language now in Chief Judge Kozinski's concurrence was seen as more advisory, or forward-looking, and not actually necessary to the Ninth Circuit's decision. Five of the eleven judges to hear this case en banc joined the Chief Judge's concurrence. *See id.* (Kozinski, J., concurring) at 1178.

[22] U.S. CONST. amend. IV.

[23] Mapp v. Ohio, 367 U.S. 643 (1961).

[24] U.S. CONST. amend. IV (emphasis added).

warrant, issued upon probable cause, that states the nature of the search and the items sought during the search.

The plain view doctrine serves as an exception to the Fourth Amendment's requirement that searches must be conducted with a warrant. In order to invoke the plain view doctrine, (1) the officer must be lawfully present at the place where the evidence can be plainly viewed, (2) the officer must have a lawful right of access to the object, and (3) the incriminating character of the object must be immediately apparent.[25] An additional requirement, that plain view evidence must be discovered *inadvertently*, was originally a part of the plain view doctrine but has since been removed.[26] A further restriction on the plain view doctrine is that law enforcement may not move or alter items in order to bring them into plain view.[27] For instance, a police officer may not turn over a stereo so that he can see its serial number and confirm that it is stolen.[28]

Federal courts enforce the Fourth Amendment's protections through the exclusionary rule. The exclusionary rule states that evidence collected or analyzed in violation of a defendant's constitutional rights shall be excluded during a criminal prosecution in a court of law.[29] The exclusionary rule does not apply to searches by a private person; it applies only to searches by government officials.[30] An extension of the exclusionary rule is the "fruit of the poisonous tree doctrine." It states that evidence obtained during an illegal government search cannot later be used to lead to other admissible evidence.[31] Thus, if the government obtains incriminating information about the defendant through an illegal search and uses the information in a second search to find other incriminating information, the government is presumptively barred from introducing the information found in the second search. To permit the admission of evidence obtained through reliance on illegally obtained evidence would encourage law enforcement to circumvent the Fourth

---

[25] *Horton*, 496 U.S. at 136-37 (known as the *Horton* test).

[26] *Id.* at 138-41.

[27] *Hicks*, 480 U.S. at 327-28.

[28] *Id.* at 327-29.

[29] United States v. Janis, 428 U.S. 433, 446-47 (1976).

[30] *See id.* at 446-48.

[31] Silverthorne Lumber Co. v. United States, 251 U.S. 385, 391-92 (1920).

Amendment.[32] To avoid the exclusion of unlawfully seized evidence, the government would have to show that the challenged evidence would inevitably have been discovered in a subsequent lawful search.[33]

III. MAJOR LEAGUE BASEBALL AND PERFORMANCE-ENHANCING DRUGS

The MLB was officially founded in 1901 and is the professional baseball league in the United States. The MLB, its owners, and its players are governed by a Collective Bargaining Agreement (the "CBA"), which outlines rules and practices governing the MLB owners and the individual players.[34] CBAs have been in effect in the MLB since 1968.[35] The past three CBAs governing the MLB ran from 1997 to 2001 (the "1997 CBA"), 2003 to 2006 (the "2003 CBA"), and 2007 to the present[36] (the "2007 CBA").

Performance-enhancing drugs ("PEDs") are substances that athletes use to gain physical or chemical advantages which lead to a competitive advantage in their sport.[37] A common form of PED is anabolic-androgenic steroids, which are used to increase muscle mass and strength.[38] Other common PEDs are androstenedione, tetrahydrogestrinone (THG) and creatine.[39] While PEDs do enhance muscle recovery, strength and energy, they pose several health risks, ranging from dehydration and hair loss to heart attack and even

---

[32] *See id.*

[33] *Id.*

[34] For the 1997 and 2003 CBAs, *see* Business of Baseball, http://roadsidephotos.sabr.org/baseball/data.htm (last visited Aug. 30, 2011); for the 2007 CBA, *see* MLBPA Info, *available at* http://mlbplayers.mlb.com/pa/info/cba.jsp.

[35] MLBPA Info, *available at* http://mlbplayers.mlb.com/pa/info/cba.jsp. The MLB was the first professional sports league to have a CBA. *Id.*

[36] The 2007 CBA is set to expire in 2011. *Id.*

[37] *See* Mayo Clinic, *Performance-enhancing drugs: Are they a risk to your health?*, http://www.mayoclinic.com/health/performance-enhancing-drugs/HQ01105 (last visited Aug. 30, 2011).

[38] *Id.*

[39] *Id.*

death.[40] The use of PEDs is illegal in the United States and banned in most professional sports leagues.[41]

Several events in the MLB led Congress to launch an investigation into the use of PEDs in the sport in the early 2000s. First, the single-season homerun record was broken twice in a three-year span: once in 1998 by Mark McGwire (seventy homeruns) and again in 2001 by Barry Bonds (seventy-three homeruns).[42] Prior to 1998, the homerun record (sixty-one homeruns) had stood since 1961.[43] These sudden challenges to the homerun record were indicative of a "power surge" that occurred during the late 1990s and early 2000s. Second, in 2005 former MLB player Jose Canseco published a "tell-all" book, *Juiced: Wild Times, Rampant 'Roids, Smash Hits & How Baseball Got Big*,[44] in which he discussed his use of steroids, as well as other players of whose steroid use he either knew or suspected.[45] Third, Ken Caminiti admitted to *Sports Illustrated* in 2002 that he used steroids and that he believed "at least half" of his fellow players used them too.[46] He died in 2004 from a heart attack at age 41.[47]

In light of these events, Congress conducted hearings and investigations, using its subpoena power to elicit the testimony of several players and prodding the MLB to get tough on steroids.[48] In

---

[40] *Id.*

[41] *Id.*

[42] Baseball-Reference.com, *Progressive Leaders & Records for Home Runs*, http://www.baseball-reference.com/leaders/HR_progress.shtml (last visited Aug. 30, 2011).

[43] *Id.*

[44] JOSE CANSECO, JUICED: WILD TIMES, RAMPANT 'ROIDS, SMASH HITS, AND HOW BASEBALL GOT BIG (William Morrow 2005).

[45] *See* Bill Nowlin, *'Juiced' Slugger Goes to Bat for Steroids*, BOSTON GLOBE, Mar. 2, 2005, *available at* http://www.boston.com/ae/books/articles/2005/03/02/juiced_slugger_goes_to_bat_for_steroids/.

[46] Tom Verducci, et al., *Totally Juiced*, SPORTS ILLUSTRATED, June 3, 2002, at 34.

[47] *How We Got Here*, *supra* note 5, at 3.

[48] *Baseball's Steroid Era: Written Steroid Era Timeline*, http://thesteroidera.blogspot.com/2006/08/baseballs-steroid-era-timeline.html (Aug. 14, 2006).

2003, the MLB instituted its first form of drug testing, and the 2003 CBA was the first to include such provisions.[49]

IV. THE GOVERNMENT RAIDS ON COMPREHENSIVE DRUG TESTING AND QUEST DIAGNOSTICS

The government, as part of its investigation into BALCO and BALCO's connection to the MLB, subpoenaed the MLB for drug testing information relating to eleven MLB players.[50] The names of these players were filed under seal and were not disclosed to the public.[51] The MLB responded that it did not possess the information requested.[52] The government reasoned that the drug testing information must be at CDT and Quest and issued subpoenas upon both organizations.[53] The original subpoenas requested drug test results for *all* MLB players tested during the 2003 season.[54] When CDT and Quest refused this request, the government obtained new subpoenas for information regarding only the eleven players they originally identified to the MLB.[55] Government investigators eventually withdrew their subpoena for one of the eleven players, thus limiting their request to ten BALCO-related targets.[56] Two days before the information requested in the subpoenas was due to federal investigators, the MLBPA filed a motion on behalf of the ten players to quash the government's subpoenas.[57]

In response to this motion, the government filed for warrants that permitted them to search CDT and Quest for the information

---

[49] *See* 2003 CBA, *supra* note 34; *see also* MLBPA Info, *supra* note 35, for a copy of the current MLB drug-testing policy, the Joint Drug Agreement.

[50] *Comprehensive Drug Testing*, 513 F.3d at 1090.

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *Comprehensive Drug Testing*, 513 F.3d at 1090 n.7.

[57] *Id.* at 1091.

requested in the subpoenas.[58] The investigators expected to find testing evidence at both locations and knew that information from one location was necessary to identify relevant records from the other location.[59] The warrants specifically authorized investigators to search for and seize the drug testing records and specimens for ten named BALCO-connected players, as well as any emails, correspondence, "manuals, pamphlets, booklets, contracts, agreements [or] other materials" which explained the administration of the MLB's drug testing program by CDT or Quest.[60] The warrants were issued in the Central District of California for the search of CDT and in the District of Nevada for the search of Quest on April 7, 2004.[61]

On April 8, federal agents executed the warrants on CDT and Quest.[62] Among the twelve investigators were Jeff Novitzky, the case's lead agent, and Joseph Abboud, a Computer Investigative Specialist.[63] At first, CDT refused to assist the investigators, telling them they should "do what they needed to do."[64] However, after agents threatened to seize all of CDT's computers, CDT agreed to help investigators by identifying "two computers on which agents would find information relevant to the search warrant."[65] CDT was clear that this assistance did not constitute consent to the government's search.[66] A document that contained drug test results for the ten named BALCO players was presented to investigators.[67] Additionally, a CDT director identified the "Tracey" directory, which contained all the files relating to CDT's drug testing program.[68] The directory

---

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *Comprehensive Drug Testing*, 513 F.3d at 1092-93.

[63] *Id.* at 1092.

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *Comprehensive Drug Testing*, 513 F.3d at 1092.

contained many subdirectories and hundreds of files, so agent Abboud recommended copying the entire directory for off-site review.[69] The warrant contemplated this situation and allowed for copying of the directory.[70]

During the CDT search, a separate set of federal agents executed their search warrant on Quest.[71] These agents were unable to locate the specimen samples contained in the warrant, as the warrant listed the players by name, but the Quest specimens were stored by number.[72] The documents collected at CDT included a list of names and identifying numbers for all MLB players, including some of the ten named in the warrant.[73] The Nevada agents received this information, obtained a new warrant for the then-known BALCO players' specimens and executed it on the evening of April 8.[74] Other documents collected at CDT, in addition to the names and identifying numbers, included a twenty-five page master list of all MLB players tested during the 2003 season and a thirty-four page list of positive drug test results.[75] Of the names listed in the thirty-four page document, eight of the ten players listed in the warrant were present; the names of twenty-six players not named in the warrant were also listed in this document.[76]

Agent Novitzky reviewed the contents of the Tracey directory upon returning to his office after the search of CDT.[77] He found five subdirectories, labeled "MAJOR LEAGUE GROUP," "MLB BILLING," "MLB Drug Subcommittee," "MLB Follow Up," and "MLB IOC," which were related to the MLB.[78] Novitzky proceeded to search these

---

[69] *Id.*

[70] *Id.* at 1092-93.

[71] *Id.* at 1093.

[72] *Id.*

[73] *Id.*

[74] *Comprehensive Drug Testing*, 513 F.3d at 1093.

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] *Id.* at 1093-94 n.20.

directories and identify files that the warrant authorized for seizure.[79] One of the files Novitzky found was the master list of all positive drug test results.[80] On April 26, the MLBPA filed a motion under FED. R. CIV. P. 41(g), seeking return of the seized property.[81] On May 5, the government applied for new search warrants to seize all specimens and records relating to more than 100 players who had tested positive for steroids.[82] Again, the government applied for warrants in both the District of Nevada and the Central District of California, since that is where Quest and CDT were located, respectively.[83] The warrants were supported by information found in the Tracey directory.[84] The courts issued the warrants, and on May 6, federal agents again raided CDT and Quest.[85] In response, the MLBPA filed more Rule 41(g) motions, seeking return of the seized specimens and records.[86]

On August 19, the District of Nevada Court granted the MLBPA's Rule 41(g) motion and ordered the return of the specimens seized and the notes compiled by the agents who reviewed the evidence, except those pertaining to the ten BALCO players named in the warrant.[87] The court found that "[t]he government callously disregarded the affected players' constitutional rights and that the government unreasonably refused [to follow the procedures set forth in *United States v. Tamura*]."[88] Approximately six weeks later, the Central District of California Court followed suit and granted the MLBPA's

---

[79] *Id.* at 1093.

[80] *Comprehensive Drug Testing*, 513 F.3d at 1093.

[81] *Id.*

[82] *Id.* at 1094.

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] *Comprehensive Drug Testing*, 513 F.3d at 1094.

[87] *Id.*

[88] *Id.* at 1094-95 (internal quotation marks omitted); *see generally* U.S. v. Tamura, 694 F.2d 591 (9th Cir. 1982).

motion.[89] That court rejected the government's contention that the computer files were seizeable under the plain view doctrine.[90]

The government appealed both of these decisions to the United States Court of Appeals for the Ninth Circuit, which consolidated the cases into *United States v. Comprehensive Drug Testing*.[91]

V. UNITED STATES V. COMPREHENSIVE DRUG TESTING CASE HISTORY

The case history of *United States v. Comprehensive Drug Testing* is unusual and illustrative of the complexity and importance of the legal issue presented. The same three-judge panel of the Ninth Circuit heard the case twice, which resulted in the original opinion being rewritten and superseded by the opinion discussed below.[92] The revised opinion was then appealed to an en banc panel of the Ninth Circuit, which issued its first opinion on August 26, 2008.[93] Upon a request for rehearing by the government, the Ninth Circuit en banc panel rescinded its original opinion and issued a similar, replacement opinion.[94] The government has stated that it will not petition for a writ of certiorari to the United States Supreme Court in this case.[95]

---

[89] *Comprehensive Drug Testing*, 513 F.3d at 1095.

[90] *Id.*

[91] *Id.* The government also appealed the decision of the District Court for the Northern District of California to quash a subpoena for the players' records. *Id.* That issue did not involve the plain view doctrine.

[92] This case was originally decided on December 27, 2006 as United States v. Comprehensive Drug Testing, 473 F.3d 915 (9th Cir. 2006). It was rescinded and reissued as United States v. Comprehensive Drug Testing, 513 F.3d 1085 (9th Cir. 2008).

[93] *Comprehensive Drug Testing*, 579 F.3d at 989 (en banc). The Ninth Circuit Court of Appeals is the largest of the 13 circuits—it covers 9 states and has 29 active judgeships. While in most jurisdictions an en banc hearing is done before all the active circuit judges, this practice is not feasible in the Ninth Circuit. As such, the Ninth Circuit Federal Rules of Appellate Procedure provide for a "limited en banc" review, in which the Chief Judge and 10 of the other 28 judges are randomly selected to rehear the case. 9TH CIR. APP. R. 35-3. The rules further allow for an en banc rehearing by the "full court." *Id.*

[94] U.S. v. Comprehensive Drug Testing, 621 F.3d 1162 (9th Cir. 2010). The new opinion stated that it "shall constitute the final action of the court. No petitions for rehearing will be considered." *Id.* at 1165.

[95] ESPN.go.com, *List of positive tests barred from courts*, http://sports.espn.go.com/mlb/news/story?id=5907927 (last visited Aug. 30, 2011).

A. UNITED STATES V. COMPREHENSIVE DRUG TESTING: *THE FIRST APPEAL*

A three-judge panel of the Ninth Circuit Court of Appeals filed its opinion on January 24, 2008. The panel reversed the district courts' decisions, finding that the government's seizure of "intermingled evidence" for off-site review pursuant to a warrant was lawful.[96] This opinion was joined by two of the three judges, with the third judge filing a dissent.[97]

The MLBPA argued that the seizure of property from Quest was unreasonable because the search warrant lacked a legally acceptable foundation.[98] The search warrant was not legally acceptable because it was based on evidence obtained from intermingled files seized at CDT, which named individuals other than the ten players originally targeted. Because these names, in the view of the MLBPA, were illegally seized, evidence discovered on the basis of their unlawful discovery should be excluded as "fruit of the poisonous tree."[99]

The court, however, rejected this argument, relying on *Tamura*, a case involving the seizure of a set of hard-copy files including target data as well as information not specified in the warrant.[100] In *Tamura*, the court ruled that the agents' seizure of files outside of the warrant was impermissible, as it effectively converted the specific warrant into a general one.[101] This conversion violated the aggrieved party's Fourth Amendment rights. The *Tamura* court identified two ways that the agents could have avoided this constitutional violation.[102] First, if the government anticipated that on-site segregation of target documents would not be feasible, it could seek a provision in the warrant to obtain intermingled documents.[103] Second, if the government

---

[96] *Comprehensive Drug Testing*, 513 F.3d. at 1116.

[97] *See id.*

[98] *Id.* at 1105.

[99] *Id.*

[100] *Id.* at 1106.

[101] *Id.*

[102] *Comprehensive Drug Testing*, 513 F.3d. at 1106.

[103] *Id.*

obtained a warrant without a protocol for removing intermingled data, but encountered an unanticipated need to seize units with intermingled data, the agents could seize these units and seal them pending post-search review authorized by the "judgment of a neutral, detached magistrate."[104] *Tamura* has since been applied to uphold the seizure of intermingled documents in the computer context.[105] In *United States v. Adjani*, the search warrant contained a detailed protocol for the seizure of intermingled evidence, thus complying with *Tamura* and the Fourth Amendment.[106]

Applying *Tamura*, the *United States v. Comprehensive Drug Testing* court found that the government's seizure of the Tracey directory was within the scope of the warrant.[107] The government agents had set forth a protocol for collecting evidence in their warrant and followed the protocol during their raid on CDT and Quest.[108] Furthermore, the agents had anticipated the necessity of off-site review and not only created a procedure for collecting the data, but also brought along a computer technician to assist with the data collection.[109] Because the Tracey directory was seized in accordance with these procedures, it was in compliance with *Tamura* and the Fourth Amendment.[110]

The court next dismissed the MLBPA's contention that the agents acted unreasonably by copying the entire Tracey directory.[111] The court discussed the difficulty in segregating intermingled electronic data, as well as the necessary balance between the government's right to investigate and seize data versus CDT's right to continue its business activities without interruption.[112] By copying the Tracey directory, the government was able to avoid seizing CDT's computers, which would

---

[104] *Id.* at 1107.

[105] *See* United States v. Adjani, 452 F.3d 1140 (9th Cir. 2006).

[106] *Id.* at 1148-50.

[107] *Comprehensive Drug Testing*, 513 F.3d at 1110-12.

[108] *Id.* at 1110.

[109] *Id.*

[110] *See id.* at 1110-11.

[111] *Id.*

[112] *Id.*

have greatly hindered CDT's ability to function as a business.[113] Thus, the court found that the government was more than reasonable in forbearing from a "wholesale seizure."[114]

The court next dismissed the MLBPA's assertion that Agent Novitzky's viewing of the data was not within the protocol of the warrant, as he was not "computer personnel."[115] The court noted that the "plain language of the search warrant did not *exclude*" Agent Novitzky from assisting with review of the data; the warrant mandated only that computer personnel determine whether "on-site segregation of target data" was feasible.[116]

Having found that the agents who searched CDT obeyed the Fourth Amendment, the court, based on the information from the search, found no grounds on which to invalidate the subsequent subpoenas and warrants.[117] Because the items in the Tracey directory were within the scope of the warrant, the court did not reach the government's plain view argument.[118]

B. UNITED STATES V. COMPREHENSIVE DRUG TESTING: *THE EN BANC DECISION*

On September 30, 2008, the Ninth Circuit Court of Appeals issued an order to rehear *United States v. Comprehensive Drug Testing* en banc[119] and ultimately reversed the panel's decision.[120] The limited en banc panel of eleven judges held that the plain view doctrine should

---

[113] *Comprehensive Drug Testing*, 513 F.3d at 1111.

[114] *Id.*

[115] *Id.*

[116] *Id.* (emphasis in original).

[117] *Id.* at 1112.

[118] *Id.* at 1112 n.48. The court did not consider the government's plain view argument, despite the fact that it was the government's sole proffered defense to its warrantless seizure of the data pertaining to the unlisted players. *See id.* at 1144 (Thomas, J., dissenting).

[119] *Comprehensive Drug Testing*, 579 F.3d 989 (en banc).

[120] *Id.*

not be applicable to computer searches and outlined a set of guidelines that judges should follow in applying this new standard.[121]

The en banc panel evaluated the government's compliance with *Tamura* in its execution of warrants on CDT and Quest.[122] The government contended that it did comply with *Tamura* and that it was not required to return any data pertaining to players not listed in the original warrant because that evidence was in plain view upon the agent's examination of the Tracey directory.[123] The court rejected this argument, emphasizing that the point of the *Tamura* procedures is to "maintain the privacy of materials that are intermingled with seizable materials and to avoid turning a *limited search* for particular information into a *general search* of office file systems and computer databases."[124] The majority noted that, under the government's proposed ruling, everything the government chose to seize would automatically come into plain view, creating a "powerful incentive to seize more rather than less."[125] The court further stated that such a ruling would "make a mockery of *Tamura*" and render its safeguards a "nullity."[126]

To avoid this "illogical result," the court suggested that the government must renounce its reliance on the plain view doctrine in digital file searches.[127] The court then laid out a set of guidelines that must be followed if the government continues to rely on the plain view doctrine, including inspection of all collected digital files by a third-party to separate seizable from non-seizable data.[128] The court advised that the process of sorting and separating seizable and non-seizable data must be designed to gather seizable data only.[129] Thus, in this case, the government would have needed to design a search protocol

---

[121] *Id.* at 1006-07.

[122] *See id.* at 997.

[123] *Id.*

[124] *Id.* at 998 (emphasis added).

[125] *Comprehensive Drug Testing*, 579 F.3d at 998 (en banc).

[126] *Id.*

[127] *Id.*

[128] *Id.* Either that, or simply refuse to issue the warrant. *Id.*

[129] *Id.* at 999.

to discover data pertaining to *only* the ten players named in the warrants, and *only* their drug test results.[130]

The court also found that the agents acted in violation of the Fourth Amendment by allowing Agent Novitzky to conduct the initial review of the Tracey directory.[131] Pursuant to the procedures in the warrant, computer personnel were to conduct the initial review of the seized data and segregate material not subject to warrant for return to the owner.[132] The government did not follow this procedure, but rather immediately sought out information on all professional baseball players in order to obtain warrants and subpoenas to further the investigation.[133] The computer analysts copied the directory, but did nothing to segregate the target data from the comingled data.[134]

The government argued that it did not violate the text or the spirit of the warrant because the warrant did not specify that *only* computer personnel could review the seized files.[135] The court rejected this argument, finding that it would make no sense to have computer personnel segregate the data if all investigatory personnel were able to review all of it in any event.[136] The court found that the government's position lacked "common sense" and that its actions constituted "deliberate overreaching. . . in an effort to seize data as to which [the government] lacked probable cause."[137]

The court proposed that, in future cases, the government include a provision in its warrants to prevent investigating agents from examining or retaining any data for which probable cause had not been shown.[138] This might require segregation to be done by an

---

[130] *Id.*

[131] *Comprehensive Drug Testing*, 579 F.3d at 999 (en banc).

[132] *Id.*

[133] *Id.* The government admitted that the idea behind taking the entire Tracey Directory was to see "if there was anything above and beyond that which was authorized for seizure in the initial warrant." *Id.*

[134] *Id.*

[135] *Id.* at 1000.

[136] *Id.*

[137] *Id.*

[138] *Id.*

independent third party.[139] Once the data have been segregated, the government agents may examine only the data within the scope of their warrant; all other data would have to be destroyed or returned to its owner.[140] The government must then provide a return disclosing exactly which data had been retained and which data had been returned.[141]

Based on its blanket denial of the plain view doctrine's applicability to computer searches, the en banc panel affirmed the district court orders, which granted CDT and the MLBPA return of the data not expressly targeted by the initial warrants.[142]

C. UNITED STATES V. COMPREHENSIVE DRUG TESTING: *THE EN BANC DECISION, TAKE TWO*

On November 4, 2009, the Ninth Circuit issued an order requesting both parties to the case to submit briefs arguing whether the case should be reheard in front of the entire Ninth Circuit Court of Appeals.[143] After briefing on the issue, the Ninth Circuit Court of Appeals en banc panel that originally decided the case rescinded its original opinion and issued a replacement opinion, in lieu of a rehearing, on September 13, 2010.[144]

Although most of the new per curium opinion is taken verbatim from the original opinion, the court did back away from its denouncement of the plain view doctrine in electronic searches and removed its advisory language on how such searches should be handled by the government.[145] The court reached the same conclusion as it did in its original opinion: it expanded the applicability of *Tamura* to digital file searches and ruled that the government had

---

[139] *Id.*

[140] *Id.*

[141] *Id.* at 1001.

[142] *Id.* at 1007.

[143] Order at 2, United States v. Comprehensive Drug Testing, No. 05-10067 (9th Cir. Nov. 4, 2009).

[144] *Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010).

[145] *See generally id.*

violated the protections of *Tamura*.[146] The court did note the complexity and importance of the issue and stated that the courts and judges must guard against over-reaching and abuse of the plain view doctrine in digital file searches by the government.[147] The advisory language on the administration of digital file searches and the denouncement of the plain view doctrine in digital file searches were moved into a concurring opinion by Chief Judge Alex Kozinski, which was joined by five of the eleven judges on the en banc panel.[148]

VI. OTHER JURISDICTIONS' APPLICATION OF THE PLAIN VIEW DOCTRINE TO DIGITAL FILE SEARCHES

Application of the plain view doctrine to government searches of computer files is a relatively new endeavor. While no court has adopted the Ninth Circuit's test or the test in Chief Judge Kozinski's concurrence, the other jurisdictions that have dealt with the issue have not reached a consensus rule either. This Part will address the other, less prominent cases where the plain view doctrine was applied to a search of digitally stored data. These decisions, while helpful in resolving this issue, provide far less analysis than *United States v. Comprehensive Drug Testing*.

A. FEDERAL CASES ADDRESSING THE APPLICABILITY OF THE PLAIN VIEW DOCTRINE TO DIGITAL SEARCHES

Besides the Ninth Circuit, courts in seven other circuits have heard at least one case relating to the plain view doctrine and electronically stored information. Four of these seven circuits—the Seventh, Eighth, Tenth, and Eleventh Circuits—have dealt with this issue at the appellate level.[149] The remaining three circuits—the Second, Third, and Fourth Circuits—have each seen a case at the district court level

---

[146] *Id.* at 1170-73.

[147] *Id.* at 1175-78.

[148] *Id.* at 1178-80. (Kozinski, C.J. concurring).

[149] *See* United States v. Mann, 592 F.3d 779 (7th Cir. 2010); United States v. Carey, 172 F.3d 1268 (10th Cir. 1999); United States v. Alexander, 574 F.3d 484 (8th Cir. 2009); United States v. Miranda, 325 F. App'x 858 (11th Cir. 2009).

relating to the plain view doctrine and electronically stored data.[150] Of these seven federal decisions, two hold that the plain view doctrine is not allowed or is severely limited in a search of electronically stored information; the remaining five decisions allow use of the plain view doctrine to admit into evidence electronically stored information obtained without a warrant.

1. FEDERAL CASES WHERE THE COURT PERMITTED THE USE OF THE PLAIN VIEW DOCTRINE TO OBTAIN ELECTRONIC DATA

In the Seventh Circuit case, *United States v. Mann*, Mann, a life guard instructor, covertly installed a video camera in a women's locker room to record footage of the women changing their clothes.[151] Two women discovered the camera and turned it over to the police. The police then executed a warrant at Mann's home and seized two desktop computers, a laptop, and an external hard drive.[152] On the seized equipment, police discovered (1) evidence that Mann had visited a website called "Perverts Are Us," where he read and possibly downloaded stories about child molestation, (2) pictures from a high school girls' locker room, (3) other child pornography, and (4) a story about a swim coach masturbating while watching young girls swim.[153]

Mann argued that the court should adopt the en banc panel's approach in *United States v. Comprehensive Drug Testing* when dealing with a computer search and seizure of evidence not directly contemplated in the warrant.[154] While the court conceded that the Ninth Circuit's approach "provide[s] some guidance," it agreed with the dissent's position that "jettisoning the plain view doctrine entirely in digital evidence cases is an efficient but overbroad approach."[155] The court *did*, however, state that those involved in searches of digital

---

[150] *See* United States v. Richardson, 583 F.Supp.2d 694 (W.D. Pa. 2008); United States v. O'Brien, 498 F.Supp.2d 520 (N.D. N.Y. 2007); United States v. Gray, 78 F.Supp.2d 524 (E.D. Va. 1999).

[151] *Mann*, 592 F.3d at 780

[152] *Id.* at 780-81.

[153] *Id.* at 781.

[154] *Id.* at 785.

[155] *Id.* (original quotations marks omitted; citing *Comprehensive Drug Testing*, 579 F.3d at 1013 (Callahan, J. concurring in part and dissenting in part)).

media should "exercise caution to ensure that warrants describe with *particularity* the things to be seized and that searches are *narrowly tailored to uncover only those things described.*"[156]

In the Eighth Circuit case, *United States v. Alexander*, Alexander had secretly videotaped women engaging in consensual sexual activity with him.[157] During a search of Alexander's residence, pursuant to a valid warrant, police found an email printout confirming subscription to a child pornography website and actual printouts of child pornography.[158] Police subsequently seized Alexander's computer and digital camera and gave them to a computer forensic analyst.[159] A search of Alexander's computer revealed child pornography.[160]

Alexander challenged the admission of the child pornography, arguing that the police exceeded the scope of their warranted search.[161] The court, using the plain view doctrine, found Alexander's claim was "without merit."[162] Because there were photographs of underage children and an email printout confirming subscription to a child pornography website in plain view, the criminal character of the computer and those items was immediately apparent.[163]

In *United States v. Miranda*, an Eleventh Circuit case, Miranda argued that police exceeded the scope of their warrant when they were looking for counterfeit software and instead found pornographic images involving minors.[164] He further argued that the image files were closed and thus were not in plain view.[165] The court noted that a search warrant must "particularly describe the place to be searched, and the persons or things to be seized."[166] The court determined,

---

[156] *Id.* at 786 (emphasis added).

[157] *Alexander*, 574 F.3d at 486.

[158] *Id.* at 487.

[159] *Id.*

[160] *Id.*

[161] *Id.* at 490.

[162] *Id.*

[163] *Id.* at 490-91.

[164] *Miranda*, 325 F. App'x at 859-60.

[165] *Id.*

[166] *Id.* at 860 (citing United States v. Khanani, 502 F.3d 1281, 1289 (11th Cir. 2007)).

however, that the particularity requirement must be "applied with a practical margin of flexibility."[167] The court found that the officers in this case were acting pursuant to a valid warrant and thus had a "lawful right to view *each file* to determine whether or not it was evidence of counterfeiting crimes."[168] Because the child pornography was intermingled with the counterfeiting files, they were in plain view.[169]

In *United States v. O'Brien*, the U.S. District Court for the Northern District of New York allowed the government to use the plain view doctrine to admit evidence obtained without a warrant.[170] O'Brien was a teacher who was accused of having inappropriate sexual relationships with some of his minor students.[171] While being interviewed by police, O'Brien admitted to having one photograph of a nude minor child on his Compaq computer.[172] When police arrived to search O'Brien's house, they noticed a Gateway computer in addition to the Compaq.[173] The police asked O'Brien if they could search the Gateway computer and O'Brien consented; the Gateway contained evidence of criminal behavior.[174]

O'Brien moved to suppress the evidence, arguing that his consent was tainted by unconstitutional police tactics.[175] The court ruled that the consent was not tainted, and in the alternative, even if it was tainted, the police could have searched the computer under the plain view doctrine.[176] The court began by noting that the officers were lawfully in a place where they could see the Gateway:[177] "The only

---

[167] *Id.* at 860.

[168] *Id.* (emphasis added).

[169] *Id.*

[170] *O'Brien*, 498 F.Supp.2d at 545.

[171] *Id.* at 526.

[172] *Id.* at 528. O'Brien later admitted to having a "few" photographs of this nature on his computer. *Id.* at 529.

[173] *Id.* at 529.

[174] *Id.* at 530, 543-45.

[175] *Id.* at 543.

[176] *Id.* at 544-45.

[177] *Id.* at 545.

issue [was] whether [the Gateway's] incriminating nature was readily apparent."*178* Based on O'Brien's past admission to the police and the Gateway's proximity to the other computer equipment, the court found that police had probable cause (a standard synonymous with "readily apparent") to search the Gateway.*179*

In *United States v. Gray*, FBI agents executed a search warrant looking for evidence of unauthorized computer intrusions ("hacking").[180] An FBI computer specialist proceeded to copy an entire hard drive onto CD-ROMs.[181] During the copying process, the computer specialist followed standard operating procedure and proceeded to open and briefly look at the files being copied, in hopes of expediting the search.[182] The computer specialist eventually stumbled upon two directories containing ".jpg" (or JPEG) files;[183] the directories were entitled "Teen" and "Tiny Teen."[184] The computer specialist viewed the files in these directories while looking for evidence of computer hacking, only to find pornographic images involving minors.[185]

The District Court for the Eastern District of Virginia noted that searches of computer files "present the same problem as document searches—the intermingling of relevant and irrelevant materials—but to a *heightened degree*."[186] The court found that searches done within the "Teen" and "Tiny Teen" directories were within the scope of the warrant, which allowed agents to search the "computer files" for evidence of computer hacking.[187] The court ruled that anything found

---

[178] *Id.*

[179] *Id.*

[180] *Gray*, 78 F.Supp.2d at 526.

[181] *Id.*

[182] *Id.*

[183] .jpg (or JPEG) are common file extensions of digitally stored photographs or picture files.

[184] *Gray*, 78 F.Supp.2d at 527.

[185] *Id.*

[186] *Id.* at 529 (citing United States v. Hunter, 13 F. Supp.2d 574, 583 (D.Vt. 1998), (emphasis added)).

[187] *Id.*

while reviewing the documents for evidence of computer hacking was within "plain view" and thus admissible against Gray.[188]

2. Federal Cases Where the Court Did Not Permit the Use of the Plain View Doctrine to Obtain Electronic Data

In *United States v. Carey*, a Tenth Circuit case, police searched Carey's home for drugs and drug paraphernalia, taking two computers in the process.[189] The warrant authorized police to search the computers for names, phone numbers, and other documentary evidence pertaining to the sale or distribution of drugs.[190] Upon searching the computers, police found several JPEGs with sexually suggestive file names.[191] The detective downloaded approximately 244 image files and opened some of them. Some of the opened files contained child pornography.[192]

Carey moved to suppress the evidence, and the government defended its acquisition of the child pornography under the plain view doctrine.[193] The court noted that "the plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."[194] Here, the warrant was limited in scope to evidence of drug trafficking.[195] The court found the plain view argument "unavailing" because the *contents* of the files and not the files *themselves* were seized; the files were closed on the computer and thus not in plain view.[196] The court did narrow its

---

[188] *Id.* at 530.

[189] *Carey*, 172 F.3d at 1270.

[190] *Id.*

[191] *Id.*

[192] *Id.* at 1271. It was necessary for the detective to use a different computer to view the JPEG files. *Id.*

[193] *Id.* at 1272-73.

[194] *Id.* at 1272 (citing *Coolidge*, 403 U.S. at 466).

[195] *Id.* at 1273.

[196] *Id. See also* United States v. Turner, 169 F.3d 84, 88 1999 WL 90209 (1st Cir.) (Sexually suggestive image suddenly coming into "plain view" does not make defendant's computer files "fair game"); United States v. Maxwell, 45 M.J. 406, 422 (U.S. Armed Forces 1996)

ruling, stating that because the officer discovered the first pornographic image inadvertently, that one image was admissible under the plain view doctrine. The subsequent pornographic images were not admissible because he then "knew or at least expected" they would contain child pornography."[197]

In *United States v. Richardson*, a case from the Western District of Pennsylvania, an Immigration and Customs Enforcement (ICE) agent searched Richardson's computer because his credit card and email address had been used in an attempt to access an illegal child pornography website.[198] Richardson recounted past occurrences of identity theft regarding his credit card, but noted that he had some past problems with child pornography.[199] The agent obtained consent to search Richardson's two computers for information about "how these [credit card] charges and allegations occurred."[200] While investigating the possibility of identity theft, the agent found child pornography on Richardson's computer.[201]

Richardson moved to suppress the evidence as a warrantless search outside the scope of his consent.[202] The government attempted to use the plain view doctrine to justify its discovery of child pornography.[203] The court found the plain view doctrine inapplicable in this case.[204] The court first noted that "government agents may not obtain consent to search on the representation that they intend to look only for certain specified items and subsequently use that consent as a license to conduct a general exploratory search."[205] Because Richardson's consent was limited to a concern for illegal credit card

---

(Child pornography found while searching a screen name not in the warrant not in "plain view").

[197] *Carey*, 172 F.3d at 1273, n.4.

[198] *Richardson*, 583 F.Supp.2d at 696-97.

[199] *Id.* at 699.

[200] *Id.* at 701.

[201] *Id.* at 704.

[202] *Id.* at 696.

[203] *Id.* at 716.

[204] *Id.*

[205] *Id.* at 715 (citing United States v. Dichiarinte, 445 F.2d 126, 129 (7th Cir. 1971)).

activity and not images, the federal agents could not rely on the plain view doctrine to admit the pornographic images; the agent was "within computer files he was not permitted" to view.[206]

B. STATE CASES ADDRESSING THE APPLICABILITY OF THE PLAIN VIEW DOCTRINE TO DIGITAL SEARCHES

Three state courts have decided cases relating to the plain view doctrine and its applicability to electronically stored information. Two courts have allowed the use of the plain view doctrine to admit electronic information seized by law enforcement without a warrant.[207] One state, Indiana, has ruled against the plain view doctrine as a basis for admitting into evidence electronically stored data seized without a warrant.[208]

1. STATE CASES WHERE THE COURT PERMITTED THE USE OF THE PLAIN VIEW DOCTRINE TO OBTAIN ELECTRONIC DATA

Massachusetts dealt with the plain view doctrine and its relation to electronically stored information in *Massachusetts v. Hinds*, where police were searching the defendant's computer for emails related to a shooting over a property dispute.[209] The officer received Hinds' consent to search his computer for "electronic mail" only.[210] While searching Hinds' computer, the officer found JPEG files entitled "10YRSLUT," "YNGSX15," "KIDSEX1," and "2BOYS.JPG."[211] The officer searching Hinds' computer had seen the "2BOYS.JPG" file in another case, and knew it to be child pornography.[212] Police seized the computer and arrested Hinds.[213]

---

[206] *Id.* at 716.

[207] Massachusetts v. Hinds, 768 N.E.2d 1067 (Mass. 2002); Missouri v. Franklin, 144 S.W.3d 355 (Mo. Ct. App. 2004).

[208] Smith v. Indiana, 713 N.E.2d 338 (Ind. Ct. App. 1999).

[209] *Hinds*, 768 N.E.2d at 1069.

[210] *Id.* at 1070.

[211] *Id.*

[212] *Id.*

[213] *Id.* at 1070.

Hinds moved to suppress the files obtained during the search of his computer.[214] The government sought to justify the seizure under the plain view doctrine.[215] The Supreme Court of Massachusetts agreed with the government.[216] It found that the titles of the files, which were in plain view in Hinds' computer directory, made the "incriminating character" of the object apparent.[217] Thus, the officer was justified in conducting further investigation and seizing the computer.[218]

In *Missouri v. Franklin*, sheriffs' deputies executed a search warrant on Franklin's home under suspicion that he was making and selling methamphetamines.[219] While searching Franklin's television room, deputies found twenty-five to thirty unmarked videotapes.[220] Deputies were aware that it was common practice for manufacturers of methamphetamines to create "instructional cooking" videos, so they proceeded to view the tapes.[221] During the process, deputies found a tape that contained images of an adult having oral and anal intercourse with a small child.[222]

Franklin contested the admission of the videotape containing child pornography into evidence, arguing that it was neither in the warrant nor in plain view.[223] The court disagreed about the evidence not being in plain view.[224] It found that because the tapes were in plain view, the deputies could inspect them.[225] The warrant provided for seizure of

---

[214] *Id.*

[215] *See id.* at 1072-73.

[216] *See id.*

[217] *Id.* at 1073.

[218] *Id.*

[219] *Franklin*, 144 S.W.3d at 357.

[220] *Id.*

[221] *Id.*

[222] *Id.*

[223] *Id.*

[224] *See id.* at 359-60.

[225] *Id.* at 359.

drug "paraphernalia," and officers frequently found tapes containing methamphetamine cooking instructions.[226] Furthermore, its incriminating character was immediately apparent, as it depicted a small child having oral and anal intercourse with an adult.[227] Thus, the tape was properly seized under the plain view doctrine.[228]

2. A State Case Rejecting the Use of the Plain View Doctrine to Obtain Electronic Data

Indiana is the lone state that has rejected the argument that the plain view doctrine applies to searches for electronically stored information. The relevant case involves the search of a cellular telephone and not a computer, but still encompasses the plain view issue. In *Smith v. Indiana*, Smith was a passenger in a car that was detained during a traffic stop.[229] During the stop, Smith consented to allow the police officer to search the vehicle.[230] The police officer seized both individuals' cellular telephones and took them back to his car.[231] By searching through the phones' internal programming and contacting the service provider, the officer discerned that the phones had illegally cloned other phones' identifying numbers.[232]

The State relied on the plain view doctrine to validate its warrantless search of the electronic contents of the cellular phones.[233] The court found, however, that merely possessing a cellular phone did not satisfy the plain view doctrine's "immediately apparent" criminal nature test.[234] The court also cited *Stanley v. Georgia*,[235] in which the

---

[226] *Id.* at 359-60.

[227] *Id.* at 360.

[228] *Id.*

[229] *Smith*, 713 N.E.2d at 345.

[230] *Id.*at 341.

[231] *Id.*

[232] *Id.*

[233] *Id.* at 345.

[234] *Id.*

[235] 394 U.S. 557 (1969).

United States Supreme Court found that the mere possession of a movie film was not "criminal activity," and officers could thus not use a projector to inspect the contents of the defendant's film to discover "previously unsuspected criminal behavior."[236] Analogizing to *Stanley*, the court suppressed the electronic cellular phone data as evidence.[237]

VII. ANALYSIS OF THE PLAIN VIEW DOCTRINE AND ITS APPLICATION TO DIGITAL FILE SEARCHES

Various federal and state courts that have reached the issue differ about exactly how to apply the plain view doctrine to searches and seizures of electronic data. Among all the approaches offered, however, the Ninth Circuit has offered the most compelling analysis. The en banc opinion in *United States v. Comprehensive Drug Testing* provides the necessary caution over using the plain view doctrine in digital file searches. Chief Judge Kozinski's concurrence goes a step further: it provides a clear, well-reasoned rule of law barring police reliance on the plain view doctrine in electronic data searches. The court's conclusion, and more so the conclusion of Chief Judge Kozinski's concurrence, is sound for three reasons: (1) it respects the importance of protecting an individual's reasonable expectation of privacy; (2) it will induce government agents to seek warrants with greater specificity; and (3) it acknowledges the simple reality that digitally stored data are not in plain view.

I would like to make an important note at the outset of the analysis. It is no coincidence that most of the cases that uphold the plain view doctrine's applicability to digital file searches involve child pornography. In the eleven case reviews above, all except *Comprehensive Drug Testing* and *Smith* involved the use of the plain view doctrine in the discovery of child pornography. An old adage in the legal community is that "bad facts make bad law." Child pornography is seen by society and the courts as a particularly reprehensible crime.[238] The justice system must find any reason it can

---

[236] *Smith*, 713 N.E.2d. at 345

[237] *Id.* at 345-46.

[238] *See* New York v. Ferber, 458 U.S. 747, 764 (1982) (Child pornography is not susceptible to the "obscenity" standard that other materials are because child pornography is per se obscene.). *See also* Osborne v. Ohio, 495 U.S. 103 (1990) (upholding a statute which makes it illegal to possess child pornography). The author of this piece also believes that possessing child pornography is opprobrious conduct, but not so opprobrious that one should lose their Fourth Amendment protections.

to admit evidence of this type of crime. Thus, a judge, faced with either excluding the evidence or admitting it using the plain view doctrine, may generally admit the evidence, even though doing so is contrary to the Fourth Amendment's express language.

Of the cases that do not allow the plain view doctrine to admit digital files, one involved professional athletes' drug test records (*United States v. Comprehensive Drug Testing*), one involved counterfeit cellular telephones (*Smith v. Indiana*), and two involved child pornography (*United States v. Carey* and *United States v. Richardson*). However, in one of the two child pornography cases that denounce the plain view doctrine in digital file searches, *United States v. Carey*, the ruling was narrow enough to admit one child pornography file into evidence because the police officer inadvertently found the file. Of the eleven cases involving the applicability of the plain view doctrine to digital file searches, nine of them involved child pornography. And of those nine, eight used the plain view doctrine to admit at least some evidence of possession of child pornography. It is hard to ignore this correlation and its affirmation that "bad facts make bad law."

A. THE PEOPLE'S EXPECTATION OF PRIVACY MUST BE PROTECTED

The Fourth Amendment guarantees to all Americans a fundamental right of privacy,[239] so long as the person seeking to invoke its protection can claim a "legitimate expectation of privacy" to be protected.[240] A legitimate expectation of privacy must be more than an idiosyncratic subjective expectation; it must be a reliance interest that society recognizes as objectively reasonable.[241] The rights created by the Fourth Amendment are so fundamental that the Court has deemed it fully incorporated as against the states through the Due Process Clause of the Fourteenth Amendment.[242]

The dissent in the *United States v. Comprehensive Drug Testing* panel opinion begins by quoting rhetorical questions posed by one of the district court judges who rejected the government's arguments:

---

[239] *Mapp*, 376, U.S. at 655.

[240] Rakas v. Illinois, 439 U.S. 128, 133-34 (1978).

[241] *Id.* at 143 n. 12.

[242] *See Mapp*, 367 U.S. 643, 655 (1961); Aguilar v. Texas, 378 U.S. 108 (1964); Ker v. California, 374 U.S. 23 (1963).

"What happened to the Fourth Amendment? Was it repealed somehow?"[243] If the plain view doctrine is applicable to electronic data searches, the government basically has the right to seize and retain anything stored in an electronic device as long as police have a warrant to look in that electronic device for any reason.[244] Such an approach would render the Fourth Amendment essentially irrelevant to electronic data searches.

The en banc panel of the Ninth Circuit that decided *United States v. Comprehensive Drug Testing* agreed that this outcome could not be in line with the Fourth Amendment.[245] They noted that if the plain view doctrine applies to electronic data, "then everything the government chooses to seize will . . . automatically" be in plain view, and thus be admissible as evidence.[246] A ruling that the plain view doctrine applies to electronic data would all but destroy a person's expectation of privacy in a computer, thus significantly endangering personal liberty. It would unnecessarily infringe on people's privacy[247] without serving the purpose of the plain view doctrine.[248] The en banc decision of the Ninth Circuit recognized these concerns and crafted its holding to ensure that individual liberty and expectations of privacy are protected.

B. THE UNAVAILABILITY OF THE PLAIN VIEW DOCTRINE WILL ENCOURAGE GREATER SPECIFICITY IN LAW ENFORCEMENT WARRANTS, IN ADHERENCE WITH THE FOURTH AMENDMENT

The Fourth Amendment states that warrants must "*particularly* describ[e] the *place* to be searched, and the persons or *things* to be seized."[249] The Supreme Court has instructed that "the plain view

---

[243] *Comprehensive Drug Testing*, 513 F.3d at 1116 (Thomas, J., dissenting).

[244] *Id.* at 1117 (Thomas, J., dissenting). *See also Gray*, 78 F. Supp.2d 524; *Miranda*, 325 Fed. Appx. 859.

[245] Comprehensive *Drug Testing*, 2010 WL 3529247 at 6.

[246] *Id.*

[247] *Carey*, 172 F.3d at 1275 (noting a greater risk of overuse of the plain view doctrine with regard to computer files than paper files because computers can inherently hold more information that is more easily accessible than a filing cabinet can).

[248] *See Coolidge*, 403 U.S. at 467 (outlining the purpose of the plain view doctrine).

[249] U.S. CONST. amend. IV (emphasis added).

doctrine may not be used to extend a general exploratory search from one object to another until something incriminating emerges."[250] Thus, it seems contrary to the Fourth Amendment's text and the Supreme Court's instruction on the plain view doctrine to allow it to expand a search to areas that are not contemplated by a warrant.

However, this is exactly what the majority of jurisdictions are allowing.[251] *United States v. Mann*, a case that upheld the plain view doctrine and directly rejected the first en banc opinion in *Comprehensive Drug Testing*, even acknowledged that those involved in searches of digital media should exercise caution to "ensure that warrants describe with *particularity* the things to be seized" and that "searches are *narrowly tailored* to uncover *only* those things described."[252] This guidance, while pertinent, is in obvious tension with the court's holding, which allows the plain view doctrine to extend to computer searches. The court's prose simultaneously suggests sympathy with the Ninth Circuit's concerns and uncertainty about embodying those concerns in a bold new doctrine.[253]

The Ninth Circuit's en banc opinion and Chief Judge Kozinski's concurrence are faithful to the Fourth Amendment. They require the government, if it wants to obtain something in a search, to ask for it during the warrant application process and show probable cause beforehand that it will be found. This is exactly what the Fourth Amendment requires.[254] The Ninth Circuit and Chief Judge Kozinski's concurrence are not writing new search and seizure law; barring law enforcement from seizing evidence without probable cause is not a new concept. Instead, the Ninth Circuit and Chief Judge Kozinski are adhering carefully to the Fourth Amendment and to Supreme Court precedent by not allowing the plain view doctrine to turn limited searches into fishing expeditions. Law enforcement officers may still search computers, but only for evidence for which they have probable cause to search.

---

[250] *Coolidge*, 403 U.S. at 466.

[251] *See O'Brien*, 498 F.Supp.2d 520.

[252] *Mann*, 592 F.3d at 786.

[253] *See id.* at 785.

[254] *Comprehensive Drug Testing*, 621 F.3d 1162, at 1168-71.

C. ITEMS DIGITALLY STORED ARE NOT IN "PLAIN VIEW" AS DEFINED BY CASE LAW

Although the plain view doctrine permits certain warrantless seizures of evidence, (1) law enforcement personnel must be lawfully present at the place where the evidence can be plainly viewed, (2) law enforcement personnel must have a lawful right of access to the object, and (3) the incriminating character of the object must be immediately apparent. The first and third parts of the *Horton* test are particularly important in addressing the plain view doctrine's use in digital file searches. In *United States v. Comprehensive Drug Testing*, the agents found the "Tracey" directory, copied it, searched it, and found the names and test results for several individuals, some of whom were named in the warrant.[255] When looking at the Tracey directory before searching it, however, no "incriminating character" could have been "immediately apparent." An unopened directory is just like a manila file folder that is full of documents. The documents inside the folder may be of interest, but they are not in plain view. Only the folder is, and it provides nothing of interest by itself. After all, it is the contents of the directory and not the directory itself that is seized and offered in issuance of subsequent warrants.[256]

An unopened file, unless labeled in a way that unambiguously indicates its criminal character, cannot meet the requirements of the plain view doctrine. The *O'Brien* and *Franklin* cases are thus prime examples of the plain view doctrine run amok. Courts in both cases reasoned that because the storage mechanism for the data was in plain view, the officers were justified in searching it.[257] By this logic, if the police can see a locked car, they can search it because the car itself is in "plain view." If they can see a house, they can search it because it is "plain view." All the police would need is some reasonable suspicion to get their collective foot in the door, and then it would be open season.[258] Although such a conclusion is obviously unsustainable, the

---

[255] *Comprehensive Drug Testing*, 513 F.3d at 1094.

[256] *See Carey*, 172 F.3d at 1273 ("The government's argument that the files were in plain view is unavailing because it is the contents of the files and not the files themselves which were seized.").

[257] *O'Brien*, 498 F.Supp.2d at 545; *Franklin*, 144 S.W.3d at 359-60.

[258] *See O'Brien*, 498 F.Supp.2d at 545; *Franklin*, 144 S.W.3d at 359-60. (Where in both cases, the courts found that since the officers had a lawful right to be in plain view of the item in which the digital information was stored, they were justified in using the plain view doctrine.).

majority of rulings with regard to the plain view doctrine and electronic searches have so far deployed similar logic.

The Ninth Circuit's en banc decision and the guidelines in Chief Judge Kozinski's concurrence provide a counterbalance to these overly-broad exercises of the plain view doctrine. Most of these computer searches deal with the distribution or possession of child pornography, which are heinous crimes. It is tempting to use the plain view doctrine to keep evidence of such a crime in the courts and to convict the culpable individuals. However, "[n]othing can destroy a government more quickly than its failure to observe its own laws,"[259] and American law says that when the state fails to obtain a warrant or lacks probable cause and incriminating items are not in plain view, the items may not be seized and used as evidence against their owner in a court of law.[260]

VII. CONCLUSION

The electronic storage of digital information poses challenges in the application of legal doctrines formulated in the pre-digital age. The applicability of the plain view doctrine to searches and seizures of electronically stored data is a clear case-in-point. The circuits are split on this issue, and the split is not merely two-sided. Besides the fundamental disagreement on whether the plain view doctrine has any role at all to play in electronic searches, even the courts holding the plain view doctrine permissible seem to differ as to the precise circumstances that make its use legitimate.

The en banc panel of the Ninth Circuit urged caution in applying the plain view doctrine in electronic search cases,[261] with the concurrence in *United States v. Comprehensive Drug Testing* denouncing the plain view doctrine in electronic searches and articulating guidelines that law enforcement should follow to avoid having searches ruled invalid and evidence suppressed under the exclusionary rule.[262] These guidelines included the segregation and redaction of files by a third-party computer technician not contemplated in the warrant, the use of carefully tailored search protocols designed to uncover only the information targeted by the

---

[259] *Mapp*, 367 U.S. at 659.

[260] *See generally Janis*, 428 U.S. 433 (explaining the exclusionary rule).

[261] *Comprehensive Drug Testing*, 2010 WL 3529247 at 1176-77.

[262] *Id.* at 1178-80. (Kozinski, C.J. concurring).

warrant, and the destruction or return of items not within the scope of the warrant.[263]

A significant split among the circuits and the growing importance of this issue strongly suggest that the Supreme Court should ultimately determine the applicability of the plain view doctrine to computer searches. If the Supreme Court grants certiorari on this issue, the Court should adopt the test as originally articulated by the Ninth Circuit en banc panel and later issued in Chief Judge Kozinski's concurring opinion. The court's holding and the concurrence's guidelines adhere to the text and spirit of the Fourth Amendment, respect citizens' rights and reasonable expectations of privacy, and limit the plain view doctrine to its logical scope.

---

[263] *Id.* at 1180 (Kozinski, C.J. concurring).